JOURNAL OF NUMBER THEORY 19, 184–194 (1984)

Evaluation of a Cubic Character Sum Using the $\sqrt{-19}$ Division Points of the Curve $Y^2 = X^3 - 2^3 \cdot 19X + 2 \cdot 19^2$

DHARAM BIR RISHI, J. C. PARNAMI, AND A. R. RAJWADE

Centre for Advanced Study in Mathematics, Panjab University, Chandigarh-160014, India

Communicated by R. P. Bambah

Received August 10, 1982

The $\sqrt{-19}$ division points on the curve $y^2 = f(x)$ of the title are calculated explicitly and the effect of the Frobenius map on these points is found in order to evaluate the cubic character sum $\sum_{x(\mathrm{mod}\ p)} (f(x)/p)$.

1. INTRODUCTION AND STATEMENT OF THE MAIN RESULT

For a polynomial $f(x)$ with integer coefficients, the character sum $\sum_{f(x)}$ is defined to be $\sum_{x(\mathrm{mod}\ p)}(f(x)/p)$, where p is a prime and (a/p) is the Legendre symbol. If $f(x)$ is linear clearly $\sum_f = 0$, and it is well known that

$$\sum_{ax^2+bx+c} = \left(\frac{a}{p}\right) \begin{cases} -1, & \text{if } b^2 - 4ac \not\equiv 0 \pmod p \\ p-1, & \text{if } b^2 - 4ac \equiv 0 \pmod p. \end{cases}$$

It is surprising that beyond this very little is known even for a cubic $f(x)$ except for some estimates. It is therefore equally remarkable that the exact value of $\sum_f$ is known for the following cubics:

$$\text{(i)}\quad x^3 + ax, \qquad \text{(ii)}\quad x(x^2 + 4ax + 2a^2), \qquad \text{(iii)}\quad x^3 + a,$$

$$\text{(iv)}\quad x(x^2 + 21ax + 112a^2), \qquad \text{(v)}\quad x^3 - 33 \cdot 32a^2x + 7 \cdot 16 \cdot 11^2a^3.$$

For the proofs of (i) see [2, 7, 11, 16], of (ii) see [1, 17, 12, 4, 6], of (iii) see [1, 10, 8, 18], of (iv) see [14], and of (v) see [13]. The common feature of these five cubics is that the curve $y^2 = f(x)$ is simply the most general elliptic curve defined over the rationals with complex multiplication respectively by $\sqrt{-1}$, $\sqrt{-2}$, $\sqrt{-3}$, $\sqrt{-7}$ and $\sqrt{-11}$. There are four other such elliptic curves and it is conjectured by E. Lehmer and R. J. Evans that in each of these cases $\sum_f$ has an answer similar to the known cases. Recently

0022-314X/84 $3.00

H. Stark has developed a method (unpublished) which evaluates these sums systematically.

The object of this paper is to treat the $\sqrt{-19}$ case. We make use of the $\sqrt{-19}$ division points on the elliptic curve with complex multiplication by $\sqrt{-19}$. Here again the major difficulty is the calculation of these division points. The relevant $f(x)$ in our case is

$$f(x) = x^3 - 2^3 \cdot 19a^2x + 2 \cdot 19^2a^3, \qquad a \in \mathbf{Z}$$

(see Hadano's list [5] of all the elliptic curves defined over the rationals admitting complex multiplications).

For this f we have (by letting $x \to ax$)

$$\sum_f = \left(\frac{a}{p}\right) \sum_{x \pmod p} \left(\frac{x^3 - 2^3 \cdot 19x + 2 \cdot 19^2}{p}\right) = \left(\frac{a}{p}\right) \mathfrak{S} \text{ (say).}$$

Our aim is the following:

THEOREM 1.

$$\mathfrak{S} = \begin{cases} 0 & \text{if } p \equiv 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19} \\ c & \text{otherwise, where } 4p = c^2 + 19d^2 \text{ where } c \text{ is} \\ & \text{determined uniquely by } (c/19) = (2/p). \end{cases}$$

2. THE $\sqrt{-19}$ DIVISION POINTS ON $y^2 = f(x)$

Let

$$y^2 = f(x) = x^3 - 2^3 \cdot 19a^2x + 2 \cdot 19^2a^3 \tag{2.1}$$

be the general elliptic curve with complex multiplication by $\sqrt{-19}$. If (x, y) is a generic point on (2.1) then it is known that [15]

$$\frac{-1 + \sqrt{-19}}{2}(x, y) = (X, Y),$$

where

$$X = \frac{\begin{array}{r}[(9+\sigma)x^5 - 2^2 \cdot 5(19+\sigma)ax^4 + 2^3 \cdot 5 \cdot 19(16-\sigma)a^2x^3 \\ - 2^5 \cdot 5 \cdot 19(57-7\sigma)a^3x^2 + 2^5 \cdot 3 \cdot 5 \cdot 19^2(6-\sigma)a^4x \\ - 2^6 \cdot 5 \cdot 19^2(19-4\sigma)a^5]\end{array}}{(-2)[5x^2 - 5(19-\sigma)ax + 2 \cdot 19(11-\sigma)a^2]^2}$$

$$Y = \frac{((1-\sigma)/4)\, y[(9+\sigma)x^6 - 2\cdot 3\cdot 5(19+\sigma)ax^5 + 2^2\cdot 11\cdot 19(9+\sigma)a^2x^4 - 2^3\cdot 19(57+73\sigma)a^3x^3 - 2^4\cdot 3\cdot 19^2(23-3\sigma)a^4x^2 + 2^5\cdot 19^2(209+\sigma)a^5x - 2^6\cdot 19^3(9+\sigma)a^6]}{[5x^2 - 5(19-\sigma)ax + 2\cdot 19(11-\sigma)a^2]^3}$$

$$(\sigma = \sqrt{-19})$$

It follows that $((-1-\sqrt{-19})/2)(x, y) = (\bar{X}, \bar{Y})$. Subtracting we get

$$\sqrt{-19}(x, y) = (X, Y) - (\bar{X}, \bar{Y}).$$

The $\sqrt{-19}$ division points on (2.1) are those (x, y) for which $\sqrt{-19}(x, y) = I$ (the point at infinity), i.e., (x, y) for which $X = \bar{X}$ or $\mathrm{Im}(X) = 0$, i.e., the (x, y) for which the x-coordinate satisfies the equation

$$x^9 - 2^2\cdot 19ax^8 + 2^2\cdot 19\cdot 23a^2x^7 - 2^5\cdot 19^2a^3x^6 - 2^5\cdot 11\cdot 19^2a^4x^5 + 2^7\cdot 3\cdot 19^3a^5x^4 - 2^9\cdot 5\cdot 19^3a^6x^3 + 2^7\cdot 3\cdot 19^4a^7x^2 - 2^8\cdot 19^4a^8x - 2^9\cdot 19^4a^9 = 0$$

and letting $x \to -2ax$ in this equation we get

$$x^9 + 38x^8 + 19\cdot 23x^7 + 4\cdot 19^2x^6 - 22\cdot 19^2x^5 - 12\cdot 19^3x^4 - 40\cdot 19^3x^3 - 3\cdot 19^4x^2 - 19^4x + 19^4 = 0. \tag{2.2}$$

If $x_1, x_2, \ldots, x_9$ are the roots of (2.2) then the 18 proper $\sqrt{-19}$ division points are $(-2ax_j, \pm y_j)$ $(j = 1, 2, \ldots, 9)$. Now it may be possible to actually prove that Eq. (2.2) has all its zeros in the maximal real subfield of $Q(\zeta)$ $(\zeta = e^{2\pi i/19})$. However, our experience with the previous cases prompts us to look for the solutions in this maximal real subfield. So let $\zeta_j = \zeta^j + \zeta^{-j}$ $(j = 1, 2, \ldots, 9)$, and let

$$x_1 = a_1\zeta_1 + a_2\zeta_2 + a_3\zeta_3 + a_4\zeta_4 + a_5\zeta_5 + a_6\zeta_6 + a_7\zeta_7 + a_8\zeta_8 + a_9\zeta_9$$

be a root of (2.2). Then the other eight roots will be the conjugates

$$x_2 = a_9\zeta_1 + a_1\zeta_2 + a_8\zeta_3 + a_2\zeta_4 + a_7\zeta_5 + a_3\zeta_6 + a_6\zeta_7 + a_4\zeta_8 + a_5\zeta_9$$

$$x_3 = a_6\zeta_1 + a_7\zeta_2 + a_1\zeta_3 + a_5\zeta_4 + a_8\zeta_5 + a_2\zeta_6 + a_4\zeta_7 + a_9\zeta_8 + a_3\zeta_9$$

$$x_4 = a_5\zeta_1 + a_9\zeta_2 + a_4\zeta_3 + a_1\zeta_4 + a_6\zeta_5 + a_8\zeta_6 + a_3\zeta_7 + a_2\zeta_8 + a_7\zeta_9$$

$$x_5 = a_4\zeta_1 + a_8\zeta_2 + a_7\zeta_3 + a_3\zeta_4 + a_1\zeta_5 + a_5\zeta_6 + a_9\zeta_7 + a_6\zeta_8 + a_2\zeta_9$$

$$x_6 = a_3\zeta_1 + a_6\zeta_2 + a_9\zeta_3 + a_7\zeta_4 + a_4\zeta_5 + a_1\zeta_6 + a_2\zeta_7 + a_5\zeta_8 + a_8\zeta_9$$

$$x_7 = a_8\zeta_1 + a_3\zeta_2 + a_5\zeta_3 + a_6\zeta_4 + a_2\zeta_5 + a_9\zeta_6 + a_1\zeta_7 + a_7\zeta_8 + a_4\zeta_9$$

$$x_8 = a_7\zeta_1 + a_5\zeta_2 + a_2\zeta_3 + a_9\zeta_4 + a_3\zeta_5 + a_4\zeta_6 + a_8\zeta_7 + a_1\zeta_8 + a_6\zeta_9$$

$$x_9 = a_2\zeta_1 + a_4\zeta_2 + a_6\zeta_3 + a_8\zeta_4 + a_9\zeta_5 + a_7\zeta_6 + a_5\zeta_7 + a_3\zeta_8 + a_1\zeta_9.$$

To find the values of the a_i's, we make use of the first two elementary symmetric functions in the x_i's. We have

$$\sum x_j = -a_1 - a_2 - a_3 - a_4 - a_5 - a_6 - a_7 - a_8 - a_9.$$

But by (2.2), $\sum x_j = -38$. Hence

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 = 38 \tag{2.3}$$

Again work out the second elementary symmetric function $\sum x_i x_j$ of x's. A straightforward calculation shows that

$$\begin{aligned}
\sum x_i x_j = &\left[\sum a_j^2 + 2\sum a_i a_j - (a_1a_2 + a_1a_9 + a_2a_4 + a_3a_6 + a_3a_8 + a_4a_8\right.\\
&\left. + a_5a_7 + a_5a_9 + a_6a_7)\right]\\
&\times (\zeta_1\zeta_2 + \zeta_1\zeta_9 + \zeta_2\zeta_4 + \zeta_3\zeta_6 + \zeta_3\zeta_8 + \zeta_4\zeta_8 + \zeta_5\zeta_7 + \zeta_5\zeta_9 + \zeta_6\zeta_7)\\
&+ \left[\sum a_j^2 + 2\sum a_i a_j - (a_3a_4 + a_2a_6 + a_3a_9 + a_4a_7 + a_5a_4 + a_6a_1\right.\\
&\left. + a_7a_2 + a_8a_5 + a_9a_8)\right]\\
&\times (\zeta_3\zeta_4 + \zeta_2\zeta_6 + \zeta_3\zeta_9 + \zeta_4\zeta_7 + \zeta_5\zeta_4 + \zeta_6\zeta_1 + \zeta_7\zeta_2 + \zeta_8\zeta_5 + \zeta_9\zeta_8)\\
&+ \left[\sum a_j^2 + 2\sum a_i a_j - (a_1a_4 + a_2a_8 + a_3a_7 + a_4a_3 + a_5a_1 + a_6a_5\right.\\
&\left. + a_7a_9 + a_8a_6 + a_9a_2)\right]\\
&\times (\zeta_1\zeta_4 + \zeta_2\zeta_8 + \zeta_3\zeta_7 + \zeta_4\zeta_3 + \zeta_5\zeta_1 + \zeta_6\zeta_5 + \zeta_7\zeta_9 + \zeta_8\zeta_6 + \zeta_9\zeta_2)\\
&+ \left[\sum a_j^2 + 2\sum a_i a_j - (a_1a_7 + a_2a_5 + a_3a_2 + a_4a_9 + a_5a_3 + a_6a_4\right.\\
&\left. + a_7a_8 + a_8a_1 + a_9a_6)\right]\\
&\times (\zeta_1\zeta_7 + \zeta_2\zeta_5 + \zeta_3\zeta_2 + \zeta_4\zeta_9 + \zeta_5\zeta_3 + \zeta_6\zeta_4 + \zeta_7\zeta_8 + \zeta_8\zeta_1 + \zeta_9\zeta_6)\\
&+ \left(\sum a_i a_j\right) \cdot \left(\sum \zeta_j^2\right).
\end{aligned}$$

Since $\zeta_i\zeta_j = \zeta_{i+j} + \zeta_{i-j}$ and $\sum \zeta_k = -1$, each sum involving the $\zeta_i\zeta_j$, in the above expression, equals -2. Thus the sum $\sum x_i x_j$ boils down to $(19/2)(228 - \sum a_j^2)$. But again by (2.2), $\sum x_i x_j = 19 \cdot 23$, hence

$$228 - \sum a_j^2 = 46 \tag{2.4}$$

Equations (2.3) and (2.4) give

$$\begin{aligned} \sum a_j &= 38 \\ \sum a_j^2 &= 182. \end{aligned} \tag{2.5}$$

One hour's calculation gives the following complete set of 14 solutions of (2.5):

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (8, 5, 5, 4, 4, 3, 3, 3, 3),$$

$$\begin{aligned} &(8, 5, 4, 4, 4, 4, 4, 3, 2), && (7, 7, 4, 4, 4, 3, 3, 3, 3), \\ &(7, 6, 6, 4, 3, 3, 3, 3, 3), && (7, 6, 5, 5, 4, 3, 3, 3, 2), \\ &(7, 6, 5, 4, 4, 4, 4, 2, 2), && (7, 6, 4, 4, 4, 4, 4, 4, 1), \\ &(7, 5, 5, 5, 5, 4, 3, 2, 2), && (7, 5, 5, 5, 4, 4, 4, 3, 1), \\ &(6, 6, 6, 5, 4, 4, 3, 2, 2), && (6, 6, 6, 4, 4, 4, 4, 3, 1), \\ &(6, 6, 5, 5, 5, 4, 3, 3, 1), && (6, 5, 5, 5, 5, 5, 4, 2, 1), \\ &(5, 5, 5, 5, 5, 5, 4, 4, 0). \end{aligned}$$

Here in each case the a_j may be combined with ζ_j in 9! ways but without loss of generality we may take $x_1 = a_1\zeta_1 + 8!$ other possibilities so that each case has 8! subcases. These are far too many to be checked for solution by computation, even on a computer. Further, consideration of the third elementary symmetric function is hopeless and may, after all, not turn out to be fruiful. We, therefore, make use of the following set of congruences which are satisfied if $x = a_1\zeta_1 + a_2\zeta_2 + a_3\zeta_3 + a_4\zeta_4 + a_5\zeta_5 + a_6\zeta_6 + a_7\zeta_7 + a_8\zeta_8 + a_9\zeta_9$ is to be a solution of (2.2):

$$\begin{aligned} \sum i^2 a_i &\equiv 0 \pmod{19} \\ \sum i^4 a_i &\equiv 0 \pmod{19} \\ \sum i^6 a_i &\equiv 0 \pmod{19} \\ \sum i^8 a_i &\not\equiv 0 \pmod{19}. \end{aligned} \tag{2.6}$$

These are derived using the following:

LEMMA. *Let* $f(x) = b_1 x + b_2 x^2 + \cdots + b_{18} x^{18}$ (b_i*'s are integers*) *and*

$\mathfrak{p} = (1-\zeta)$ *be the ideal generated by* $1-\zeta$ *in* $Q(\zeta)$, $\zeta = e^{2\pi i/19}$. *Then* $\mathfrak{p}^8 \| f(\zeta)$ *iff* $f(1) \equiv f^{(1)}(1) \equiv \cdots \equiv f^{(7)}(1) \equiv 0 \pmod{19}$ *and* $f^{(8)}(1) \not\equiv 0 \pmod{19}$.

Proof. Write $f(x) = a_0 + a_1(1-x) + \cdots + a_{18}(1-x)^{18}$. The result follows using the facts that $\mathfrak{p}^{18} = (19)$ and $\mathfrak{p} \mid b$, $b \in \mathbf{Z}$ iff $19 \mid b$.

Now to prove set (2.6) of congruences, let $f(\zeta) = a_1\zeta_1 + a_2\zeta_2 + \cdots + a_9\zeta_9$ be a solution of (2.2). Then notice that in $Q(\zeta)$, $(\text{norm } (f(\zeta))) = (19^8) = \mathfrak{p}^{144}$ and therefore $\mathfrak{p}^8 \| f(\zeta)$. Use the above lemma and get, in particular,

$$f^{(2)}(1) \equiv f^{(4)}(1) \equiv f^{(6)}(1) \equiv 0 \pmod{19} \qquad \text{and} \qquad f^{(8)}(1) \not\equiv 0 \pmod{19}$$

(the other congruences of the lemma are in fact redundant) which give the required congruences.

With the constraints given by (2.6), the computer sorts out only two 9-tuples, namely $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (7, 4, 4, 4, 2, 5, 2, 6, 4)$ and $(7, 5, 6, 3, 4, 2, 3, 3, 5)$ from all the possible 8! permutations each from the fourteen 9-tuples mentioned earlier. Of these two the first one works out to be the right one. Hence we find that the 9 roots of (2.2) are

$$x_1 = 7\zeta_1 + 4\zeta_2 + 4\zeta_3 + 4\zeta_4 + 2\zeta_5 + 5\zeta_6 + 2\zeta_7 + 6\zeta_8 + 4\zeta_9$$

and the conjugates $x_2, x_3, x_4, x_5, x_6, x_8, x_9$ are found by letting $\zeta \to \zeta^j$ $(j = 2, 3, 4, 5, 6, 7, 8, 9)$ in x_1. This then gives the following:

PROPOSITION 1. *The x-coordinates of the proper* $\sqrt{-19}$ *division points on* (2.1) *are*

$$X_1 = -2ax_1 = -2a(7\zeta_1 + 4\zeta_2 + 4\zeta_3 + 4\zeta_4 + 2\zeta_5 + 5\zeta_6 + 2\zeta_7 + 6\zeta_8 + 4\zeta_9)$$

$$X_2 = -2ax_2 = -2a(4\zeta_1 + 7\zeta_2 + 6\zeta_3 + 4\zeta_4 + 2\zeta_5 + 4\zeta_6 + 5\zeta_7 + 4\zeta_8 + 2\zeta_9)$$

$$X_3 = -2ax_3 = -2a(5\zeta_1 + 2\zeta_2 + 7\zeta_3 + 2\zeta_4 + 6\zeta_5 + 4\zeta_6 + 4\zeta_7 + 4\zeta_8 + 4\zeta_9)$$

$$X_4 = -2ax_4 = -2a(2\zeta_1 + 4\zeta_2 + 4\zeta_3 + 7\zeta_4 + 5\zeta_5 + 6\zeta_6 + 4\zeta_7 + 4\zeta_8 + 2\zeta_9)$$

$$X_5 = -2ax_5 = -2a(4\zeta_1 + 6\zeta_2 + 2\zeta_3 + 4\zeta_4 + 7\zeta_5 + 2\zeta_6 + 4\zeta_7 + 5\zeta_8 + 4\zeta_9)$$

$$X_6 = -2ax_6 = -2a(4\zeta_1 + 5\zeta_2 + 4\zeta_3 + 2\zeta_4 + 4\zeta_5 + 7\zeta_6 + 4\zeta_7 + 2\zeta_8 + 6\zeta_9)$$

$$X_7 = -2ax_7 = -2a(6\zeta_1 + 4\zeta_2 + 2\zeta_3 + 5\zeta_4 + 4\zeta_5 + 4\zeta_6 + 7\zeta_7 + 2\zeta_8 + 4\zeta_9)$$

$$X_8 = -2ax_8 = -2a(2\zeta_1 + 2\zeta_2 + 4\zeta_3 + 4\zeta_4 + 4\zeta_5 + 4\zeta_6 + 6\zeta_7 + 7\zeta_8 + 5\zeta_9)$$

$$X_9 = -2ax_9 = -2a(4\zeta_1 + 4\zeta_2 + 5\zeta_3 + 6\zeta_4 + 4\zeta_5 + 2\zeta_6 + 2\zeta_7 + 4\zeta_8 + 7\zeta_9).$$

Now substitute for X_1 in (2.1) and we get the corresponding y-coordinate as $Y_1 = a\sqrt{-38a}\,[355\zeta_1 + 91\zeta_2 + 207\zeta_3 + 271\zeta_4 + 51\zeta_5 + 379\zeta_6 + 19\zeta_7 + 323\zeta_8 + 147\zeta_9]^{1/2}$. Let $X = 355\zeta_1 + 91\zeta_2 + 207\zeta_3 + 271\zeta_4 + 51\zeta_5 + 379\zeta_6 + 19\zeta_7 + 323\zeta_8 + 147\zeta_9$. We expect $X^{1/2}$ to belong to $\mathbf{Z}[\zeta]$. In case it does not,

we still have the $\sqrt{-38}$ outside to fiddle with; it may be that $(-X)^{1/2}$ or $(\pm 2X)^{1/2}$ or $(\pm 19X)^{1/2}$ or $(\pm 38X)^{1/2}$ may lie in $\mathbf{Z}[\zeta]$. Trying for these various possibilities we see that $(-19X)^{1/2}$ works; i.e.,

$$(-19X)^{1/2} = c_1\zeta_1 + c_2\zeta_2 + c_3\zeta_3 + c_4\zeta_4 + c_5\zeta_5 + c_6\zeta_6 + c_7\zeta_7 + c_8\zeta_8 + c_9\zeta_9$$

with $c_j \in \mathbf{Z}$ is solvable and we want to determine the c_j. Squaring and equating coefficients we get the following system of Diophantine equations:

$$\begin{aligned}
&(C_1 - C_2)^2 + (C_2 - C_3)^2 + (C_3 - C_4)^2 + (C_4 - C_5)^2 + (C_5 - C_6)^2 \\
&\qquad + (C_6 - C_7)^2 + (C_7 - C_8)^2 + (C_8 - C_9)^2 + C_1^2 = 6745 \\
&(C_2 - C_3)^2 + (C_4 - C_6)^2 + (C_6 - C_8)^2 + (C_8 - C_9)^2 + (C_9 - C_7)^2 \\
&\qquad + (C_7 - C_5)^2 + (C_5 - C_3)^2 + (C_3 - C_1)^2 + C_2^2 = 1729 \\
&(C_3 - C_6)^2 + (C_6 - C_9)^2 + (C_9 - C_7)^2 + (C_7 - C_4)^2 + (C_4 - C_1)^2 \\
&\qquad + (C_1 - C_2)^2 + (C_2 - C_5)^2 + (C_5 - C_8)^2 + C_3^2 = 3933 \\
&(C_4 - C_8)^2 + (C_8 - C_7)^2 + (C_7 - C_3)^2 + (C_3 - C_1)^2 + (C_1 - C_5)^2 \\
&\qquad + (C_5 - C_9)^2 + (C_9 - C_6)^2 + (C_6 - C_2)^2 + C_4^2 = 5149 \\
&(C_5 - C_9)^2 + (C_9 - C_4)^2 + (C_4 - C_1)^2 + (C_1 - C_6)^2 + (C_6 - C_8)^2 \\
&\qquad + (C_8 - C_3)^2 + (C_3 - C_2)^2 + (C_2 - C_7)^2 + C_5^2 = 969 \qquad (2.7) \\
&(C_6 - C_7)^2 + (C_7 - C_1)^2 + (C_1 - C_5)^2 + (C_5 - C_8)^2 + (C_8 - C_2)^2 \\
&\qquad + (C_2 - C_4)^2 + (C_4 - C_9)^2 + (C_9 - C_3)^2 + C_6^2 = 7201 \\
&(C_7 - C_5)^2 + (C_5 - C_2)^2 + (C_2 - C_9)^2 + (C_9 - C_3)^2 + (C_3 - C_4)^2 \\
&\qquad + (C_4 - C_8)^2 + (C_8 - C_1)^2 + (C_1 - C_6)^2 + C_7^2 = 361 \\
&(C_8 - C_3)^2 + (C_3 - C_5)^2 + (C_5 - C_6)^2 + (C_6 - C_2)^2 + (C_2 - C_9)^2 \\
&\qquad + (C_9 - C_1)^2 + (C_1 - C_7)^2 + (C_7 - C_4)^2 + C_8^2 = 6137 \\
&(C_9 - C_1)^2 + (C_1 - C_8)^2 + (C_8 - C_2)^2 + (C_2 - C_7)^2 + (C_7 - C_3)^2 \\
&\qquad + (C_3 - C_6)^2 + (C_6 - C_4)^2 + (C_4 - C_5)^2 + C_9^2 = 2793.
\end{aligned}$$

In (2.7) by expanding the squares in the first equation, we find that c_1 is odd. Similarly looking at the other equations we infer

(i) All c_i's are odd.

Again if $(c_1, c_2, \ldots, c_9)$ is a solution of (2.7) then so is $(-c_1, -c_2, \ldots, -c_9)$. Therefore:

(ii) Without loss of generality we can take any one of the c_i's to be positive.

(iii) Immediate bounds can be given to c_i's from the equations in (2.7), e.g., the first equation implies $c_1^2 \leqslant 6745$ giving $-82 \leqslant c_1 \leqslant 82$.

(iv) A solution of (2.7) also satisfies the conditions given by (2.6).

Now keeping the above conditions in view, we solve the tiresome system (2.7) of diophantine equations on a computer and get

$$(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9) = (35, 7, 23, 29, 3, 39, -1, 25, 11)$$

as a solution. Since there is a unique solution (upto sign), this gives $-19X = (35\zeta_1 + 7\zeta_2 + 23\zeta_3 + 29\zeta_4 + 3\zeta_5 + 39\zeta_6 - \zeta_7 + 25\zeta_8 + 11\zeta_9)^2$. This may be directly checked. We have proved the following:

PROPOSITION 2. *The y-coordinates of the* $\sqrt{-19}$ *division points on* (2.1) *are respectively*

$$Y_1 = (2a)^{1/2} \cdot a[35\zeta_1 + 7\zeta_2 + 23\zeta_3 + 29\zeta_4 + 3\zeta_5 + 39\zeta_6 - \zeta_7 + 25\zeta_8 + 11\zeta_9]$$

$$Y_2 = (2a)^{1/2} \cdot a[11\zeta_1 + 35\zeta_2 + 25\zeta_3 + 7\zeta_4 - \zeta_5 + 23\zeta_6 + 39\zeta_7 + 29\zeta_8 + 3\zeta_9]$$

$$Y_3 = (2a)^{1/2} \cdot a[39\zeta_1 - \zeta_2 + 35\zeta_3 + 3\zeta_4 + 25\zeta_5 + 7\zeta_6 + 29\zeta_7 + 11\zeta_8 + 23\zeta_9]$$

$$Y_4 = (2a)^{1/2} \cdot a[3\zeta_1 + 11\zeta_2 + 29\zeta_3 + 35\zeta_4 + 39\zeta_5 + 25\zeta_6 + 23\zeta_7 + 7\zeta_8 - \zeta_9]$$

$$Y_5 = (2a)^{1/2} \cdot a[29\zeta_1 + 25\zeta_2 - \zeta_3 + 23\zeta_4 + 35\zeta_5 + 3\zeta_6 + 11\zeta_7 + 39\zeta_8 + 7\zeta_9]$$

$$Y_6 = (2a)^{1/2} \cdot a[23\zeta_1 + 39\zeta_2 + 11\zeta_3 - \zeta_4 + 29\zeta_5 + 35\zeta_6 + 7\zeta_7 + 3\zeta_8 + 25\zeta_9]$$

$$Y_7 = (2a)^{1/2} \cdot a[25\zeta_1 + 23\zeta_2 + 3\zeta_3 + 39\zeta_4 + 7\zeta_5 + 11\zeta_6 + 35\zeta_7 - \zeta_8 + 29\zeta_9]$$

$$Y_8 = (2a)^{1/2} \cdot a[-\zeta_1 + 3\zeta_2 + 7\zeta_3 + 11\zeta_4 + 23\zeta_5 + 29\zeta_6 + 25\zeta_7 + 35\zeta_8 + 39\zeta_9]$$

$$Y_9 = (2a)^{1/2} \cdot a[7\zeta_1 + 29\zeta_2 + 39\zeta_3 + 25\zeta_4 + 11\zeta_5 - \zeta_6 + 3\zeta_7 + 23\zeta_8 + 35\zeta_9].$$

Now let P be the $\sqrt{-19}$ division point (X_1, Y_1). Then all the 18 proper $\sqrt{-19}$ division points are $\pm jP$, $j = 1, 2, \ldots, 9$. We further need to know which is which. A simple calulation involving addition of points on (2.1) gives finally the following:

THEOREM 2. *Let* X_j *and* Y_j $(j = 1, 2, \ldots, 9)$ *be as found in Propositions* 1 *and* 2. *Then the proper* $\sqrt{-19}$ *division points* (18 *in number*) *on the elliptic curve* (2.1) *are* $(X_j, \pm Y_j)$. *If* P *is the point* (X_1, Y_1) *then* $2P = (X_4, -Y_4)$, $3P = (X_9, -Y_9)$, $4P = (X_3, Y_3)$, $5P = (X_6, Y_6)$, $6P = (X_2, Y_2)$, $7P = (X_8, Y_8)$, $8P = (X_7, -Y_7)$, $9P = (X_5, Y_5)$ *and of course for any point* (X, Y) *one has* $-(X, Y) = (X, -Y)$.

3. Proof of Theorem 1

Let N_p be the number of points on the projective curve

$$y^2 = x^3 - 2^3 \cdot 19Z^2x + 2 \cdot 19^2Z^3$$

in the finite field of p elements. First of all, $N_p = 1 +$ the number of solutions of the congruence $y^2 \equiv x^3 - 2^3 \cdot 19x + 2 \cdot 19^2 \pmod{p}$ (the 1 coming from the point at infinity)

$$= 1 + \sum 1 + \left(\frac{y^2}{p}\right) = p + 1 + \mathfrak{S}$$

(the $\mathfrak{S}$ mentioned in Theorem 1) (3.1)

But by a well known theorem of Deuring's [3] we have

$$N_p = \begin{cases} p+1, & \text{if } p \text{ is not a norm from } Q(\sqrt{-19}) \text{ to } Q, \\ p+1-\pi-\bar{\pi}, & \text{otherwise, where } p = \text{Norm } \pi = \pi\bar{\pi}. \end{cases}$$

Let $\pi = (c + d\sqrt{-19})/2$, $c \equiv d \pmod 2$. Then $p = \pi\bar{\pi} = (c^2 + 19d^2)/4$, i.e., $4p = c^2 + 19d^2$ and $\pi + \bar{\pi} = c$. Hence Deuring's theorem gives

$$N_p = \begin{cases} p+1, & \text{if } p \equiv 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19}, \\ p+1-c, & \text{otherwise, where } 4p = c^2 + 19d^2. \end{cases} \tag{3.2}$$

Equating (3.1) and (3.2) gives

$$\mathfrak{S} = \begin{cases} 0, & \text{if } p \equiv 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19} \\ -c, & \text{otherwise, i.e., if } p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}. \end{cases} \tag{3.3}$$

Here the problem is the sign of c, i.e., the normalization of π and $\bar{\pi}$. Deuring's theorem also tells us that the correct sign $+\pi$ or $-\pi$ is that for which multiplication of points of (2.1) by the π with the correct sign has the same effect as has the Frobenius automorphism

$$f_p : (x, y) \to (x^p, y^p) \pmod{p}.$$

We try the action of the Frobenius automorphisms on the $\sqrt{-19}$ division point $\underline{P} = (X_1, Y_1)$ of Theorem 2 with $a = 1$ for $p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$ successively.

Case 1. $p \equiv 1 \pmod{19}$. We have $f_p(\underline{P}) = (X_1^p, Y_1^p) = (X_1, (2/p)Y_1) = (2/p)(X_1, Y_1)$. But $f_p(\underline{P}) = \pi\underline{P}$ by the very definition of π with the correct sign. Hence $(\pi - (2/p))\underline{P} = \underline{I}$. But $\underline{P}$ is a proper $\sqrt{-19}$ division point, and it follows that $\pi \equiv (2/p) \pmod{\sqrt{-19}}$, i.e., $c + d\sqrt{-19} \equiv 2(2/p) \pmod{\sqrt{-19}}$, i.e., $-c \equiv 17(2/p) \pmod{19}$.

Case 2. $p \equiv 4 \pmod{19}$. Then $f_p(\underline{P}) = (X_1^p, Y_1^p) = (X_4, (2/p)Y_4) = (2/p)(X_4, Y_4) = (2/p)(-2\underline{P})$ (see Theorem 2). Hence as above $\pi \equiv -2(2/p) \pmod{\sqrt{-19}}$ giving $-c \equiv 4(2/p) \pmod{19}$ and similarly

Case 3. $p \equiv 5 \pmod{19}$. Here $-c \equiv (2/p) \pmod{19}$.

Case 4. $p \equiv 6 \pmod{19}$. Here $-c \equiv 9(2/p) \pmod{19}$.

Case 5. $p \equiv 7 \pmod{19}$. Here $-c \equiv 16(2/p) \pmod{19}$.

Case 6. $p \equiv 9 \pmod{19}$. Here $-c \equiv 6(2/p) \pmod{19}$.

Case 7. $p \equiv 11 \pmod{19}$. Here $-c \equiv 5(2/p) \pmod{19}$.

Case 8. $p \equiv 16 \pmod{19}$. Here $-c \equiv 11(2/p) \pmod{19}$.

Case 9. $p \equiv 17 \pmod{19}$. Here $-c \equiv 7(2/p) \pmod{19}$.

Hence by (3.3)

$$\mathfrak{S} = \begin{cases} 0 & \text{if } p \equiv 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19}, \\ c & \text{otherwise where } 4p = c^2 + 19d^2 \end{cases}$$

with

$$c \equiv \left(\frac{2}{p}\right) \cdot \begin{cases} 17 \\ 4 \\ 1 \\ 9 \\ 16 \\ 6 \\ 5 \\ 11 \\ 7 \end{cases} \pmod{19} \text{ according as } p \equiv \begin{cases} 1 \\ 4 \\ 5 \\ 6 \\ 7 \\ 9 \\ 11 \\ 16 \\ 17 \end{cases} \pmod{19},$$

i.e., $(c/19) = (2/p)$. This completes the proof of Theorem 1.

ACKNOWLEDGMENTS

We take this opportunity to give our most sincere thanks to Mr. Vinod Parnami of Regional Computer Centre, Chandigarh for his invaluable help on the computer in solving Eq. (2.2) and the set of Diophantine equations (2.7).

REFERENCES

1. B. W. BREWER, On certain character sums, *Trans. Amer. Math. Soc.* **99** (1961), 241–245.
2. H. DAVENPORT AND H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen, *Crelle* **172** (1934), 151–182.
3. M. DEURING, Die Typen den Multiplikatorenrings Elliptische Funktionen Korper, *Zbh. Math. Sem. Univ. Hamburg* **14** (1941), 197–272.
4. R. E. GUIDICI, J. B. MUSKAT, AND S. F. ROBINSON, On the evaluation of Brewer's character sums, *Trans. Amer. Math. Soc.* **171** (1972), 317–347.
5. T. HADANO, Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor, *Proc. Japan Acad.* **51** (1975), 92–95.
6. P. A. LEONERD AND K. S. WILLIAMS, Jacobi sums and a theorem of Brewer, *Rocky Mountain J. Math.* **5** (1975), 301–308; erratum, **6** (1976), 501.
7. B. MORLAYE, Demonstration elementaire d'un theorems de Davenport et Hasse, *Enseign. Math.* **18** (1972), 269–276.
8. L. D. OLSON, Conductors of elliptic curves, *J. Number Theory*, **8** (1976), 397–414.
9. A. R. RAJWADE,Arithmetic on curves with complex multiplication by the Eisenstein integers, *Proc. Cambridge Philos. Soc.* **65** (1969), 59–73.
10. A. R. RAJWADE, On rational primes p congruent to 1 (mod 3 or 5), *Proc. Cambridge Philos. Soc.* **66** (1969), 61–70.
11. A. R. RAJWADE, A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - Dx \pmod{p}$, *Proc. Cambridge Philos. Soc.* **67** (1970), 603–605.
12. A. R. RAJWADE, Certain classical congruences via elliptic curves, *J. London Math. Soc.* **8** (1974), 60–62.
13. A. R. RAJWADE AND J. C. PARNAMI, A new cubic character sum, *Acta Arith.* **40** (1982), 347–356.
14. A. R. RAJWADE, The Diophantine equation $y^2 = x(x^2 + 21D + 112D^2)$ and the conjectures of Birch and Swinnerton–Dyer, *J. Austral. Math. Soc.* **24** (1977), 286–295.
15. DHARAM BIR RISHI, J. C. PARNAMI, AND A. R. RAJWADE, Complex multiplication by $(1 + \sqrt{-19})/2$, *Indian J. Pure Appl. Math.* **14** (1983), 630–634.
16. SURJIT SINGH AND A. R. RAJWADE, The number of solutions of the congruence $y^2 \equiv x^4 - a \pmod{p}$, *Enseign. Math.* **20** (1974), 265–273.
17. A. L. WHITEMAN, A theorem of Brewer on Character sums, *Duke Math. J.* **30** (1963), 545–552.
18. K. S. WILLIAMS, Note on a cubic character sum, *Acquationes Math.* **12** (1975), 229–231.